UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,300	11/30/2000	Alain Pomet	99RO21154217	4083

7590 06/06/2007

CHRISTOPHER F. REGAN, ESQUIRE
ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST, P.A.
P.O. Box 3791
Orlando, FL 32802-3791

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
06/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/727,300	POMET ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *12-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *12-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the arguments filed on 15 March 2007.

2. Claims 12-49 are pending in the application.

3. Claims 12-49 have been rejected.

4. Claims 1-11 have been cancelled.

Response to Arguments

5. Applicant's arguments filed 15 March 2007 have been fully considered but they are not persuasive.

On page 16, the applicant argues that Carmeli fails to show that the data bus and the transmission line are separated from one another, as shown in figure 2 of the applicant's specification.

The examiner respectfully disagrees. As shown, for example, in figure 4, there is shown a schematic illustration of a system for protecting a trusted network 32 from a hostile, or non-trusted network 30, constructed and operative in accordance with one embodiment of the present invention. The system includes a slave unit 34 coupled to the hostile network 30, and a master unit 36 coupled to the trusted network 32. Slave unit 34 includes an SBC 40 and a wide bus gate card 42. Master unit 36 includes an SBC 46 and a wide bus gate card 44. Slave unit 34 is coupled for communication to master unit 36 via a wide bus 38. It will be appreciated that, in this way, hostile network 30 is physically isolated at all times from trusted network 32. The slave unit would be connected to the hostile unit through a transmission line and the master unit is coupled to the trusted network through a transmission line. The slave unit and the master unit are coupled for communication through a separate wide bus.

On pages 16 and 17, the applicant argues that no transmission line, distinct from the computer bus 28, can be identified in the slave or master unit of Carmeli between the SBC 22 and the wide bus gate card 24, which could be used to provide a synchronous random signal to each section 22 and 24 or the master or slave unit for the production of the common secret key.

The examiner respectfully disagrees. As discussed above, there is a separate transmission line that is distinct from the data bus. Carmeli discloses that the functions of the master unit (in this case, the receiver) and the slave unit (in this case, the sender) are shown in FIGS. 7a, 7b, 7c, and 7d. First, the master SBC 46 sends an import request to the master wide bus gate card 44 (FIG. 7a, block 50). When master wide bus gate card 44 receives an import request message (FIG. 7b, block 52), the master wide bus gate card 44 sends a request to the slave wide bus gate card 42 for that file (FIG. 7b, block 58). When the slave wide bus gate card receives the request (FIG. 7d, block 56), it forwards the request to the slave SBC 40 (FIG. 7d, block 60). These requests can be signed, and/or coded, and/or encrypted, as desired. When slave SBC 40 receives the import request from wide bus gate card 42 (FIG. 7c, block 54), slave SBC 40 reads the entire required data from where it is currently stored (FIG. 7c, block 62), and builds data header record (FIG. 7c, block 64). The header is a fixed size record that contains information about the data such as its age, size, where it was stored, etc. The data header can include additional parameters, such as communication information. In addition, the header includes the original location (source) and destination address. The most important field in the data header is the signature, which is computed by slave SBC 40 (FIG. 7d, block 66). Without a signature, no data can be used in the network in which it is received. According to a preferred embodiment of the invention, the signature is a large number (e.g., 1024 bits long), that "describes" the specific

collection of bytes that are stored inside the header record and the entire data content. One example of static data to be transported, including its header, is shown schematically in FIG. 8. It is generated from both the file header and content bytes. Preferably, building the signature is based on a special function that takes a secret key and a stream of bytes consisting of the data header and the data content bytes, and as a result generates the signature number. This function is a very fast one. Both the SBC and the wide bus gate cards know the secret key value and, thus, a secret key transaction over the computer bus is not necessary. The examiner asserts that the synchronous signal is provided through the transmission line for production of the secret key. Carmeli specifically discloses that both the SBC and the wide bus gate cards know the secret key value and, thus, a secret key transaction over the computer bus is not necessary.

On pages 17 and 18, the applicant argues that Carmeli fails to disclose a transmission line distinct from the bus 28 that is used to transmit a synchronous random signal to each section 22, 24, from which the common secret key would be produced. The applicant argues that on contrary, the random values used to produce the secret key common to each section are transmitted on the computer bus at the time of starting.

The examiner respectfully disagrees. See the above explanation.

On page 18, the applicant argues that the modification of the current value of the secret key is not controlled by the clock signal contrary to the claimed invention.

The examiner respectfully disagrees. Carmeli discloses using the system clock with the random number generator.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 12-16, 18, 19, 21-26, 28, 29, 31-35, 37, 38, 40-44, 46, 47 and 49 are rejected under 35 U.S.C. 102(e) as being anticipated by Carmeli U.S. Patent No. 6,865,672 B1.

As to claims 12, 25, 34 and 42, Carmeli discloses an electronic device comprising:

a central processing unit [column 5 line 65 to column 6 line 18];

at least one peripheral device [column 5 line 65 to column 6 line 18];

a data bus connected between the at least one peripheral device and the central processing unit through which data travels at a rate of a clock signal [column 9, lines 13-25]; and

a transmission line connected between the at least one peripheral device and the central processing unit for providing a random signal thereto that is synchronous with the clock signal [column 9, lines 13-25];

the central processing unit and the at least one peripheral device each comprising a data encryption/decryption cell connected to the data bus and to the transmission line for generating a same current secret key at each clock cycle based upon the random signal [column 9 line 54 to column 10 line 12].

As to claims 13 and 43, Carmeli discloses that the at least one peripheral device comprises a memory [column 5 line 65 to column 6 line 18].

As to claim 14, Carmeli discloses that the same current secret key changes at each successive clock cycle [column 9 line 54 to column 10 line 12].

As to claims 15, 26, 35 and 44, Carmeli discloses that each data encryption/decryption cell comprises a shift register having an input for receiving the random signal and an input for receiving the clock signal, and an output for providing the same current secret key at each clock cycle [column 9 line 54 to column 10 line 12].

As to claim 16, Carmeli discloses that the shift register comprises a feedback type shift register [column 10, lines 42-52].

As to claims 18, 28, 37 and 46, Carmeli discloses that each data encryption/decryption cell comprises:

> an encryption module having an input for receiving the secret key and an input for receiving the data to be transmitted, and an output for providing encrypted data [column 16, lines 10-32]; and
>
> a decryption module having an input for receiving the secret key and an input for receiving the data, and an output for providing decrypted data [column 16, lines 10-32].

As to claims 19, 29, 38 and 47, Carmeli discloses that the data encryption/decryption cell of the central processing unit further comprises a conditional circuit for applying the secret key or a neutral key to the encryption and decryption modules based upon an encryption enabling signal [column 16, lines 10-32].

As to claims 21, 31 and 40, Carmeli discloses that the encryption module and the decryption module each operate based upon a same mathematical function [column 16, lines 10-32].

As to claims 22 and 32, Carmeli discloses that a random signal generator connected to the transmission line for generating the random signal that is synchronous with the clock signal [column 9 line 54 to column 10 line 12]. Carmeli suggests that the random signal generator further comprises a consumption masking circuit [column 9 line 54 to column 10 line 12].

As to claims 23, 33 and 41, Carmeli discloses that the random signal generator comprises a D-type flip-flop having an input for receiving a random binary signal and an input for receiving the clock signal and an output for providing the random signal [column 9 line 54 to column 10 line 12]. Carmeli discloses that the consumption masking circuit is connected between the output of the D-type flip-flop circuit and the transmission line [column 9 line 54 to column 10 line 12].

As to claim 24, Carmeli discloses that a value of the same current secret key on the transmission line is set to zero by default by the central processing unit [column 9 line 54 to column 10 line 12]. Carmeli discloses that the random signal generator comprises a logic circuit to transmit the random signal on the transmission line after activation of a control signal by the central processing unit [column 9 line 54 to column 10 line 12].

As to claim 49, Carmeli discloses that the random signal is generated by a random signal generator connected to the transmission line [column 9 line 54 to column 10 line 12].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 17, 27, 36 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carmeli U.S. Patent No. 6,865,672 B1 as applied to claims 12, 25, 34 and 42 above, and further in view of Finkelstein U.S. Patent No. 6,014,446.

As to claims 17, 27, 36 and 45, Carmeli does not teach that the shift register performs a polynomial function based upon n most recent values of the random signal.

Finkelstein teaches a shift register that performs a polynomial function based upon the most recent values of the random signal [column 4 line 60 to column 5 line 27].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Carmeli so that the shift register would have performed a polynomial function based upon the most recent values of the random signal.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Carmeli by the teaching of Finkelstein because by using complex polynomials, it makes the encryption functions less vulnerable to attacks [column 2, lines 17-30].

8. Claims 20, 30, 39 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carmeli U.S. Patent No. 6,865,672 B1 as applied to claims 12, 25, 34 and 42 above, and further in view of Smyth et al U.S. Patent No. 6,058,481.

As to claims 20, 30, 39 and 48, Carmeli teaches a peripheral access control circuit connected to the central processing unit, as discussed above.

Carmeli does not teach that the at least one peripheral device generates the encryption enabling signal based upon an address of the at least at least one peripheral device.

Smyth et al teaches a peripheral device that generates an encryption enabling signal based upon an address of the at least at least one peripheral device [column 3, lines 32-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Carmeli so that a peripheral device would have generated a encryption enabling signal based upon an address of the at least at least one peripheral device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Carmeli by the teaching of Smyth et al because it provides a high degree of security to prevent unauthorized access to files and ensures that a minimum level of encryption is needed [column 2, lines 13-22].

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy AM
June 1, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100